NEL REPORT 1152

AN ELECTRONIC GENERATOR OF RANDOM NUMBERS

G. M. Dillard and R. E. Simmons • Research and Development Report 1152 • 21 December 1962

U. S. NAVY ELECTRONICS LABORATORY, SAN DIEGO, CALIFORNIA • A BUREAU OF SHIPS LABORATORY

THE PROBLEM

Develop new radar techniques, based upon statistical methods, which are applicable to automatic radar systems with increased detection capabilities. The specific phase reported here is the construction and statistical evaluation of an electronic generator of random numbers which is used in laboratory experiments, evaluation of radar detector performance by Monte Carlo methods, and in simulation of physical phenomena.

RESULTS

An electronic generator of random numbers has been constructed and evaluated. This random number generator has been used to generate a sequence of ones and zeros with a predetermined probability of a one in the evaluation of an experimental sequential detector. The device has also been used to generate random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at NEL.

RECOMMENDATIONS

Consider the RNG suitable for application to digital systems requiring the use of random numbers.

ADMINISTRATIVE INFORMATION

Work was performed under SF 001 02 05, Task 6072 (NEL D1-17, formerly NEL D1-9), BUSHIPS letter C-9670/2 ser 684-B-028 of 12 June 1962. The report covers one aspect of experimental and analytical work accomplished from January 1960 to January 1962, and was approved for publication 21 December 1962.

The authors wish to acknowledge many valuable discussions with J. W. Caspers regarding the RNGs and are also indebted to R. D. Strait and A. L. Sullivan, who designed and constructed the thyratron noise generators and noise-controlled pulse generators used in the RNG system.

In the course of preparing this report it came to the attention of the authors that a similar device for generating random numbers was discussed in a paper by Jan Havel.[1] (See list of references at end of report.)

CONTENTS

TABLES

ILLUSTRATIONS

INTRODUCTION

The random number generator (RNG) described in this report generates 14-bit random numbers at a 15-kc/s rate. All 14 bits are generated simultaneously, each bit being generated by a separate sub-unit. The RNG was developed to be used in conjunction with an experimental sequential detector constructed at the U. S. Navy Electronics Laboratory.[2] A sequence of ones and zeros with a predetermined probability description was needed as an input to the detector. This binomial sequence was generated by comparing the output of the RNG with a preset 14-bit binary number. Subsequently the RNG output has been used in the process of generating random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at the Navy Electronics Laboratory.[3] This report describes the generation of the random numbers, discusses the statistical evaluation of the RNG, briefly describes how the first application mentioned above was made, and mentions possible other uses of such a device.

MONTE CARLO METHODS

Various numerical calculations can be carried out with the use of random numbers. The term "Monte Carlo" is usually applied to any such calculations. As an example, suppose it is desired to find the value of $\int_0^1 f(x)dx$, where $0 \le f(x) \le 1$. This value can be estimated by setting up a stochastic process involving a random variable y, with the property that $E(y) = \int_0^1 f(x)dx$, where $E(y)$ is the expected value of y. Some sort of sampling procedure would yield the estimate. One method of sampling would be as follows: From a set of random numbers uniformly distributed in the interval (0, 1), draw two samples s and t. If $y = 1$ for $f(s) \ge t$, and $y = 0$ otherwise, then $E(y) = \int_0^1 f(x)dx$.

Monte Carlo methods can also be applied to the evaluation of characteristics of tests of statistical hypotheses. For example, suppose x is a random variable with frequency function $f(x, \theta)$, and it is desired to test the hypothesis $H_0 : \theta = \theta_0$ against the alternative $H_1 : \theta = \theta_1$. Observations are to be made on the random variable x, and some criterion is established by which either H_0 or H_1 is accepted (e.g., the Neyman-Pearson test). Let $k_m(H_0)$ and $k_m(H_1)$ be the number of times out of m tests that H_0 and H_1 respectively are accepted. For large m, when $\theta = \theta_0$, then $\alpha \approx k_m(H_1)/m$; and when $\theta = \theta_1$ then $\beta \approx k_m(H_0)/m$, where α and β are the probabilities of type I and type II errors, respectively. If the number, n, of observations required in each test is a random variable (e.g., sequential tests), and if N is the total number of observations required for m tests, then $E(n) \approx N/m$.

These are only two of many applications of Monte Carlo methods. Other applications include: estimation of collisions involving neutrons or other particles, solution of differential and integral equations, and the inversion of matrices.

SEQUENTIAL DETECTOR EVALUATION BY MONTE CARLO METHODS

The second example mentioned above suggested evaluating the characteristics of tests of statistical hypotheses by Monte Carlo methods. It was for this purpose that the random number generator was developed. A sequential detector to detect signal in the presence of noise in radar video was to be evaluated. The video was quantized into two levels, one and zero; hence the detector was a "binomial sequential detector."[2] It was assumed that when only noise was present the probability of observing a 1 was p_0 and when both signal and noise were present the probability of observing a 1 was p_1. A Wald sequential probability ratio test[4] was to be used to test the hypothesis $H_0: p = p_0$ against the alternate $H_1: p = p_1$. The detector characteristics were evaluated by Monte Carlo methods utilizing the random number generator. This required generating a sequence $\{x_i\}$, where $x_i = 1$ or $x_i = 0$, such that Prob $\{x_i = 1\} = p$, where p is the parameter of the binomial distribution considered. The method for generating this sequence will be described later.

Briefly, the operation of the detector was as follows: An accumulator was loaded initially with a quantity D_0 $(0 \leq D_0 \leq 1)$. For each 1 observed, a quantity $D_s (0 \leq D_s \leq 1)$ was added to the contents of the accumulator. If the contents of the accumulator were then greater than or equal to 1, H_1 was accepted; if not, another observation was made. For each 0 observed, a quantity $D_f (0 \leq D_f \leq 1)$ was subtracted from the contents of the accumulator. If the contents of the accumulator were less than or equal to zero, H_0 was accepted; if not, another observation was made. Hence, after initially loading the accumulator with D_0, observations were made until one of the hypotheses was accepted. By repeating this process a large number of times for each of several different values of p (p = Prob $\{x_i = 1\}$) and for each of several different values of D_0, D_s, and D_f, the detector characteristics were evaluated. A complete description of the detector and its evaluation is found in reference 2.

DESCRIPTION OF RNG EQUIPMENT

A block diagram of the random number generator (RNG) is shown in figure 1. The RNG generates a 14-bit binary number with the property that the probability is $\frac{1}{2}$ that any particular bit is a 1. Also each bit is independent

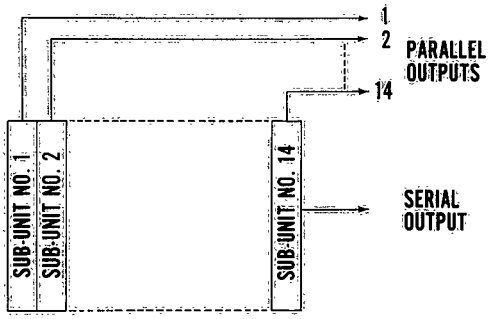

Figure 1. Block diagram of the random number generator.

of all other bits; i.e., each bit is generated by a separate sub-unit. The output of the RNG is either serial or parallel depending of the particular application to be made of the output. The output of the RNG can be considered to be a sequence of integers uniformly distributed in the interval $[0, 2^{14} - 1]$ such that, for each observation x_i, Prob $\{x_i = k\} = 2^{-14}$ for $k = 0, 1, \ldots 2^{14} - 1$. A detailed description of the RNG follows.

The RNG was constructed from commercial plug-in type digital modules together with laboratory developed and constructed modular-type pulse generators. The digital modules utilize dynamic circuitry and operate synchronously with respect to a 1-Mc/s clock frequency; i.e., the "one" state is a 1-Mc/s train of -3 volt pulses and the "zero" state is 0 volt dc. The modules are compatible

with inputs from other modules operating at the clock frequency, and with inputs of dc voltages. For example, a gate with a dc input of -3 volts will assume the "one" state. Figure 2 shows the relationship between a gate output and its input. It should be noted that, although a particular type of logic device is discussed, an RNG of this type need not be restricted to their use.

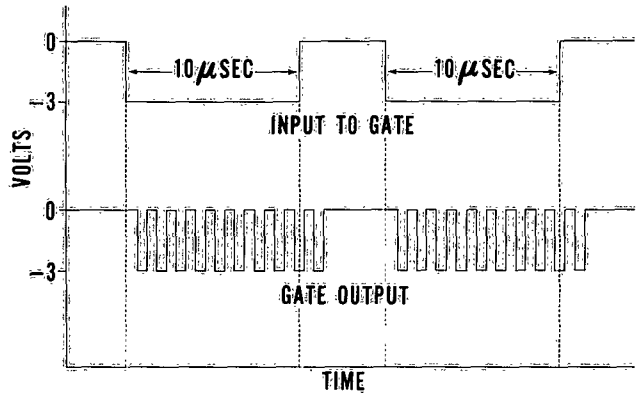

Figure 2. Relationship between a gate output and its input.

Details of Operation

Figure 3 is a block diagram of a typical sub-unit, fourteen of which constitute the RNG. Figure 4 is a diagram of the pulse relationships of the various components of a typical sub-unit, figure 5 is a photograph of a thyratron noise generator and random-width-pulse generator module, and figure 6 is a photograph of the complete RNG.

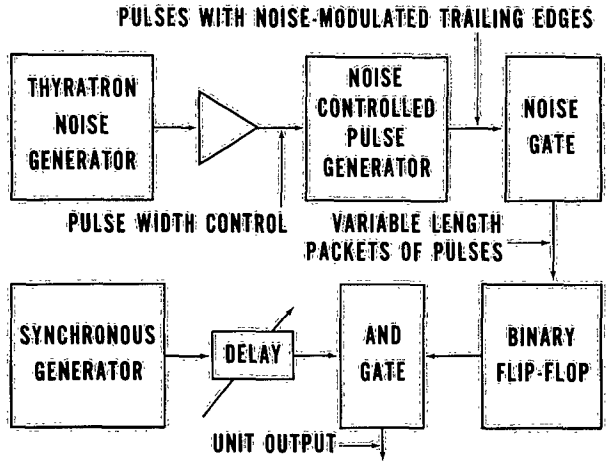

Figure 3. Block diagram of a typical sub-unit.

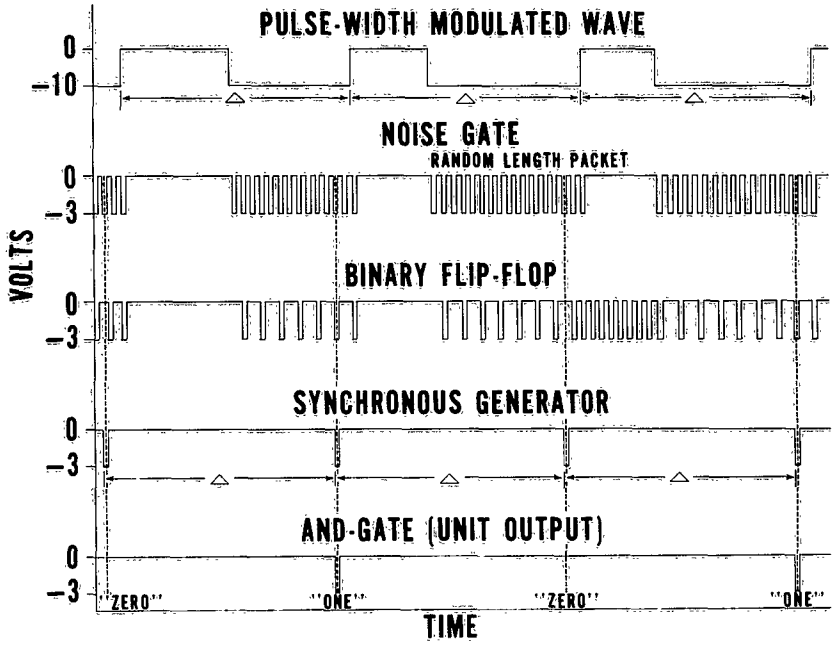

Figure 4. Pulse relationships of the components of a typical sub-unit.

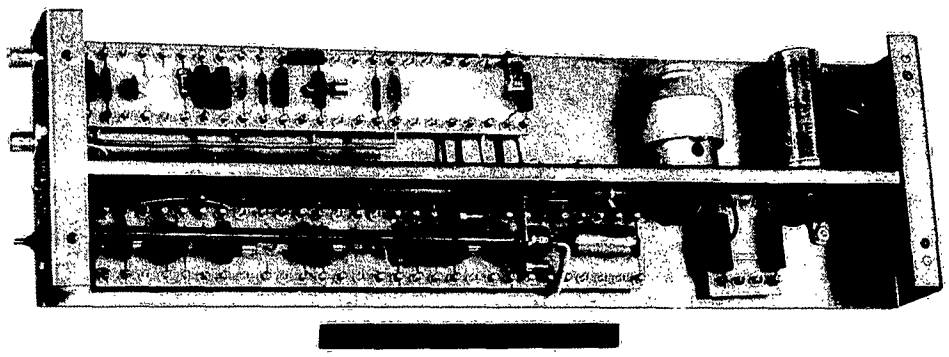

Figure 5. Thyratron noise generator and random-width-pulse generator.

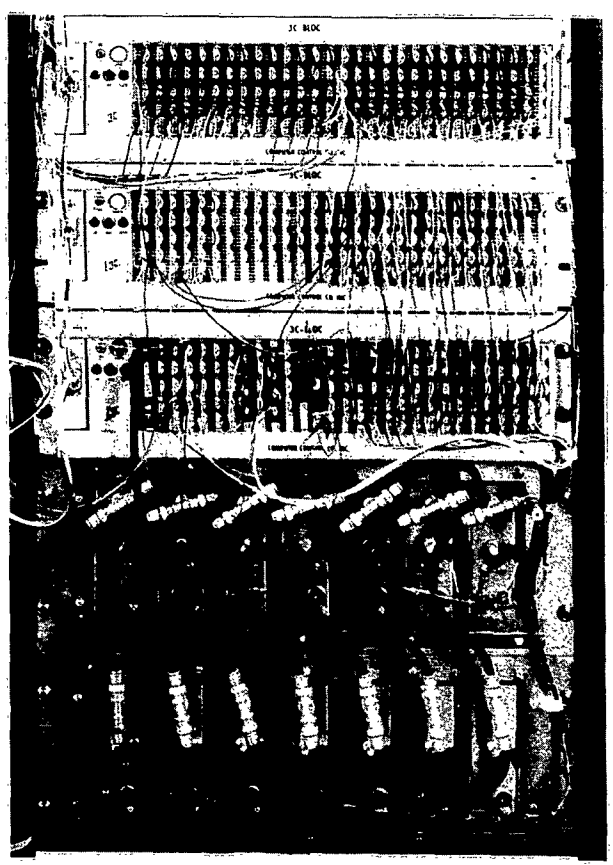

Figure 6. The complete random number generator.

The following description refers to one of the fourteen sub-units which constitute the RNG. The output of a thyratron noise generator is amplified and used to control the pulse width of a pulse generator. The output of the noise-controlled-pulse generator is a pulse-width modulated wave of positive pulses (referenced to -10 volts) with their leading edges occurring at 15 kc/s. The pulse width varies randomly between fixed limits, the maximum width depending on the maximum modulation applied. The pulse-width variation about the mean is approximately symmetric. The pulse-width modulated wave is applied to a gate which is "on" during the interpulse period as indicated in figure 4. Since the leading edges of the noise-modulated pulses occur at fixed intervals and the pulse widths vary randomly, the interpulse durations also vary randomly. Hence the output of the gate to which the pulse-width modulated wave is applied is a succession of random-length packets of 1-Mc/s pulses. These packets trigger a binary flip-flop which changes state following each input pulse. At the end of each packet the flip-flop may be in either state, one or zero, and the flip-flop is not reset before the arrival of the next packet of pulses. If the flip-flop is reset between packets, any bias toward an even or odd number of pulses in a packet shows up as a bias in the number of zeros or ones upon sampling the flip-flop. In order to smooth out this effect, the flip-flop is not reset between packets; it remains in its prior state until the next packet arrives. An analysis of this smoothing effect is given in the appendix. In order to sample the state of the flip-flop, the output of the flip-flop is AND-gated with a synchronous generator pulse occurring at 15 kc/s. The synchronous generator pulse is delayed in such a manner that it appears before the flip-flop stops. This procedure is used to avoid any bias which might result from a tendency of the flip-flop to assume a particular state, particularly as a result of "pulse splitting" which might occur on the last pulse of a packet. The output of the AND-gate will be a one or zero depending on the state of the flip-flop at the time of arrival of the synchronous generator pulse. This AND-gate output is the output of one sub-unit of the RNG; the simultaneous output from all 14 sub-units constitutes the RNG output.

Although a technique for generating random binary digits has been described, the method can obviously be extended to generate numbers to any integral base n ($n \geq 2$). The random width pulses are applied to an AND-gate together with the output of a clock of period t seconds, the product tn being small compared with the smallest possible random width pulse. The output of this gate will be a series of packets of pulses, each packet containing a random number of clock pulses. Since the product tn is small with respect to the smallest possible random-width pulse, the probability that a packet of pulses will contain $k \pmod n$ pulses ($k = 0, 1, \ldots, n-1$) is approximately $1/n$. Hence, if the event "$k \pmod n$ pulses in a packet" is called the digit k ($k = 0, 1, \ldots, n-1$), the output of the AND-gate will be a sequence of random digits with approximately equal probabilities of occurrence. In order to transform the generated sequence into usable form, the AND-gate output is applied to a counter (mod n) and the state of the counter is sampled in the interval between packets of pulses. The n possible states of the counter will be identified with the digits $0, 1, \ldots, n-1$ in such a manner that 0 corresponds to 0 (mod n) pulses in a packet, 1 corresponds to 1 (mod n) pulses in a packet, etc. For generating random binary digits the counter takes the form of a simple flip-flop as previously described; for decimal digits a decade counter would suffice.

Quantizing the RNG Output

As mentioned earlier, the motivation for developing the RNG was to evaluate a binomial sequential detector by Monte Carlo methods.[2] The detector input was required to be a sequence of ones and zeros with a predetermined (fixed) probability of a one. This detector input was generated in the following manner. The RNG output, R, was compared serially in a comparator C, with a preset (fixed) number Q. If $R > Q$, then the output of C was a one; otherwise the output was a zero. Since 2^{14} binary numbers

were equally likely as an output from the RNG, the fixed number Q was chosen in such a manner that Prob $\{C = 1\}$ took any fixed value which was a multiple of 2^{-14} and was between zero and one. The output of the comparator C was taken as the input to the detector.

TESTS FOR RANDOMNESS

To test the randomness of the RNG, four tests analogous to those used by Kendall and Smith[5] were applied to the output of each of the fourteen sub-units. Also independence between sub-units was tested in a manner to be described below.

The simplest randomness test is the frequency test. This consists of counting the total number of ones in a given sample. We expect the number of ones to be one-half of the total sample size.

The serial test checks the tendency of a one to be followed by a one or by a zero, etc. This test is performed by sampling in pairs. We expect the pairs (1, 1), (1, 0), (0, 1), and (0, 0) to occur equally often.

If we sample the output of a sub-unit in blocks of three, for example, then we expect one-eighth of the total number of triples to contain no ones, three-eighths to contain a single one, three-eighths to contain two ones, and one-eighth to contain three ones. This type of test is called the poker test.

The last test applied to the output of each sub-unit is the gap test. It is performed by choosing an arbitrary binary digit, say a one, and then counting the number of times a one is followed by a one, by a zero and then a one, by two zeros and then a one, and so on. In other words, we check zero gap, one gap, two gap; etc. We expect zero gap to occur one-half the time, one gap to occur one-fourth the time, etc.

Independence between sub-units is tested by simultaneously sampling the output of two or more of the sub-units. If the outputs of two sub-units are sampled simultaneously, then we expect the ordered pairs (0, 0), (0, 1), (1, 0), and (1, 1) all to occur equally often. This is similar to the serial test, except that here each member of the observed pairs is the output from each of two different sub-units. A similar situation results if three or more of the sub-units are sampled simultaneously.

A further test of independence is performed by quantizing the 14-bit number at a certain level Q as previously described. Upon choosing Q, the probability of a one from the output of the quantizer (comparator) is fixed and the expected frequency of ones is known.

The output of the RNG was also indirectly tested for randomness. As mentioned earlier, the quantized output from the RNG was used as the input to an experimental binomial sequential detector. For many of the tests performed on the experimental detector, exact analytical computations furnished theoretical results. The results of the Monte Carlo methods were in excellent agreement with the theoretical results.

The χ^2 test, which was used throughout, tests the goodness of fit of the observed frequencies to the expected frequencies. The symbol χ_q^2 is used to indicate the computed χ^2 value with q degrees of freedom. The symbol P is used for Prob$\{ \chi^2 \geq \chi_q^2 \}$, and p^* is used to indicate the sample mean. The statistic for the serial test was changed from that used by Kendall and Smith[5] to the statistic indicated by I. J. Good.[6]

RESULTS OF TESTS

Table 1 shows the results of the serial test on the output of one sub-unit of the random number generator. The expected number of pairs for each entry in the table is 2500. The data for the frequency test are easily obtained from the same data, and the results of this test are included in the table. The expected number of observed ones in each row is 5000. The sample mean, p^*, is given for the indicated columns.

Table 1. Serial test (pairs) and frequency test. Ten blocks, 10,000 pairs in each block.

	Pairs						Obs. Ones		
	(1,1)	(1,0)	(0,1)	(0,0)	X_1^2	P		X_1^2	P
	2502	2495	2495	2508	0.040	.84	4997	0.004	.95
	2544	2508	2508	2440	0.102	.75	5052	1.082	.30
	2460	2524	2524	2492	0.923	.34	4984	0.102	.75
	2503	2499	2499	2569	0.002	.96	4932	1.850	.17
	2539	2502	2502	2457	0.806	.35	5041	0.672	.41
	2498	2539	2539	2424	2.434	.12	5037	0.548	.46
	2556	2499	2499	2446	0.002	.96	5055	1.210	.27
	2512	2462	2462	2564	2.310	.13	4974	0.270	.60
	2547	2465	2465	2523	1.960	.16	5012	0.058	.81
	2467	2496	2496	2541	0.538	.46	4963	0.292	.59
Total	25058	24989	24989	24964	0.019	.89	50047	0.088	.77
p^*	.25058	.24989	.24989	.24964			.50047		

Table 2 shows the results of the poker test applied to quadruples from the output of one sub-unit of the random number generator. In each row the expected number of quadruples containing no ones or four ones is 1024, the expected number containing a single one or three ones is 4096, and the expected number containing two ones is 6144. Again the data for the frequency test are obtained from the same data, and the results of this test are included in the table. The expected number of observed ones in each row is 32,768.

Table 2. Poker test (quadruples) and frequency test. Ten blocks, 16,384 quadruples in each block.

	Number of ones in quadruple							Obs.		
	0	1	2	3	4	X_4^2	P	Ones	X_1^2	P
	1010	4199	6096	4051	1028	3.667	.45	32656	0.766	.38
	1060	4121	6124	4081	998	2.198	.70	32604	1.642	.20
	1071	4068	6120	4058	1067	4.601	.33	32750	0.020	.89
	990	4070	6212	4122	990	3.341	.50	32820	0.165	.68
	997	4128	6168	4052	1039	1.748	.60	32776	0.004	.95
	1058	4157	6081	4076	1012	2.922	.56	32595	1.827	.18
	1002	4067	6106	4144	1065	3.117	.54	32971	2.515	.11
	1053	4000	6034	4274	1023	12.777	.01	32982	2.795	.09
	1021	4103	6091	4145	1024	1.064	.90	32816	0.141	.71
	1026	4154	6149	4037	1018	1.714	.79	32635	1.080	.30
Total	10288	41067	61181	41040	10264	1.807	.77	327605	0.034	.85
*p**	.06279	.25065	.37342	.25049	.06265			.499886		

Table 3 shows the results of the gap test applied to the output of one sub-unit of the random number generator. The expected number of zero gaps is 8192, the expected number of one gaps is 4096; etc. No frequency test results are available from these data.

Table 3. Gap test.

Length of gap						
0	1	2	3	≥4	X_4^2	P
8238	4102	2046	1006	992	1.585	.81
8175	4118	2097	1011	983	3.132	.55
8165	4134	2035	1036	1014	0.762	.94
8246	4130	2012	1012	984	2.974	.56
8094	4132	2089	1045	1024	2.740	.60
8041	4129	2090	1044	1080	7.364	.12
8187	4091	2048	1037	1021	0.174	.99
8117	4083	2060	1063	1061	3.620	.46
8194	4072	2065	994	1059	2.357	.67
8205	4057	2045	1020	1057	1.475	.83
Total 81662	41048	20587	10268	10275	1.757	.78
*p** .49843	.25054	.12565	.06267	.06271		

Table 4 shows results of an independence test between two sub-units of the random number generator. The method for obtaining the data is described previously. The expected number of pairs for each entry in the table is 4096.

Table 4. Independence test between two units. Ten blocks, 16, 384 pairs in each block.

	Pairs					
	(1,1)	(1,0)	(0,1)	(0,0)	X_3^2	P
	4123	4172	3985	4104	4.611	.20
	4078	4162	3990	4154	4.707	.20
	4106	4151	4021	4106	2.161	.55
	4068	4054	4073	4189	2.862	.40
	4156	4025	4063	4140	2.848	.40
	4130	4166	4024	4064	2.994	.38
	4128	4046	4122	4088	1.041	.80
	4199	4041	4117	4027	4.598	.20
	4031	4112	4145	4096	1.680	.65
	3983	4092	4250	4059	9.245	.03
Total	41002	41021	40790	41027	0.949	.82
p^*	.25026	.25037	.24896	.25041		

Table 5 shows results of quantizing the 14-bit binary numbers from the random number generator. The quantizing level used is such that the probability of a one is the binary fraction .01010101010101 which has a decimal equivalent of approximately .3333129883. Hence the expected number of ones in each block is 5461 and the expected number of zeros is 10, 923.

Table 5. Quantization of 14-bit number.
Ten blocks, 16,384 observations in each block.

	Ones	Zeros	X_1^2	P
	5366	11018	2.479	.12
	5412	10972	0.659	.42
	5340	11044	4.021	.04
	5528	10856	1.233	.27
	5490	10894	0.231	.63
	5446	10938	0.062	.80
	5547	10837	2.031	.15
	5472	10912	0.033	.86
	5552	10832	2.274	.13
	5466	10918	0.0069	.93
Total	54619	109221	0.00222	.96
p^*	.3333679	.6666321		

Table 6 shows the results obtained from Monte Carlo evaluation of the binomial sequential detector mentioned earlier, for the particular values of D_0, D_s, and D_f indicated. $E(n)$ is the expected number of observations for a single test, $L(p)$ is the probability of accepting the null hypothesis (H_0) when p has a particular value, and p is the probability of observing a one. Data for the columns headed "Exact" were obtained by analytical computations and the columns labelled "Exp." contain the experimental results.

Table 6. Results of Monte Carlo evaluation of the binomial sequential detector for $D_0 = 1/2$, $D_f = 1/32$, and $D_s = 1/8$.

p	$E(n)$ Exact	Exp.	$L(p)$ Exact	Exp.
.03125	18.9626	18.9150	1.00000	1.0000
.0625	23.2574	23.4211	.99968	.9997
.09375	29.8781	30.1512	.99612	.9957
.125	40.3776	40.1545	.97390	.9744
.140625	47.4225	47.1290	.94163	.9439
.15625	55.2351	55.2084	.88108	.8787
.171875	62.5432	62.6890	.78143	.7819
.1875	67.3192	67.8328	.64248	.6483
.203125	67.8640	68.0311	.48309	.4729
.21875	64.1653	64.2987	.33333	.3452
.234375	57.8193	56.9864	.21499	.2204
.25	50.6929	50.9022	.13264	.1319
.28125	38.2019	38.2154	.04746	.0473
.3125	29.4568	29.4924	.01662	.0145
.34375	23.5890	23.7319	.00583	.0064
.375	19.5505	19.5183	.00205	.0018
.40625	16.6562	16.8974	.00072	.0008

CONCLUSIONS

The results of the statistical tests gave no reason for rejecting the hypothesis that the 14-bit numbers generated by the random number generator are uniformly distributed. Also, excellent agreement with theory was obtained in Monte Carlo evaluation of an experimental binomial sequential detector.

REFERENCES

1. Havel, J., "An Electronic Generator of Random Sequences," p. 219-229 in Conference on Information Theory, Statistical Decision Functions, Random Processes; Second, Transactions, Prague, Czechoslovak Academy of Sciences, 1960

2. Navy Electronics Laboratory Report 999, An Experimental Sequential Detector, by G. M. Dillard and R. E. Simmons, 8 November 1960

3. Navy Electronics Laboratory Report 1021, TBD - A New Long-Range Radar Surveillance System, by J. W. Caspers and others, CONFIDENTIAL, 3 May 1961

4. Wald, A., Sequential Analysis, Wiley, 1947

5. Kendall, M. G. and Smith, B. B., "Randomness and Random Sampling Numbers," Royal Statistical Society, Journal, v. 101, p. 147-166, 1938

6. Good, I. J., "The Serial Test For Sampling Numbers and Other Tests For Randomness," Cambridge Philosophical Society, Proceedings, v. 49, p. 276-284, 1953

APPENDIX: ANALYSIS OF "NOT RESETTING" FLIP-FLOP

We assume that initially the flip-flop is in the zero state and is not reset after being triggered by a packet. Let p be the probability that a packet has an odd number of pulses and p_k be the probability that the flip-flop is in the one state after having been triggered by k packets. We note that $p_0 = 0$ and $p_1 = p$.

Now
$$p_k = (1-p)p_{k-1} + p(1-p_{k-1})$$

$$= (1-2p)p_{k-1} + p$$

The general solution of this difference equation is

$$p_k = \tfrac{1}{2} + c(1-2p)^k$$

Since $p_0 = 0$, we have $c = -\tfrac{1}{2}$.

Therefore

$$p_k = \tfrac{1}{2}(1-(1-2p)^k)$$

Let

$$p = \tfrac{1}{2} + \epsilon, \quad |\epsilon| < \tfrac{1}{2}$$

then

$$p_k = \tfrac{1}{2}(1-(-2\epsilon)^k)$$

and

$$\lim_{k\to\infty} p_k = \tfrac{1}{2}$$

Thus we see that if p differs from $\frac{1}{2}$, by taking k large enough p_k will be as close to $\frac{1}{2}$ as is desired. This is the motivation for not resetting the flip-flop after each packet. Closer examination of the above analysis reveals however that "not resetting" is not a "cure-all." An undesirable situation exists if $|\epsilon|$ is not very small. If we assume k large enough so that $p_k \approx \frac{1}{2}$, then Prob $\{(1,1)\}$ = Prob $\{(0,0)\}$ = $\frac{1}{2}(\frac{1}{2} - \epsilon)$ and Prob $\{(1,0)\}$ = Prob $\{(0,1)\}$ = $\frac{1}{2}(\frac{1}{2} + \epsilon)$.

Thus if $|\epsilon|$ is not very small the probabilities associated with pairs will be severely biased. To take an extreme example let $\epsilon = \frac{1}{2}$. Then $p_k = \frac{1}{2}(1 - (-1)^k)$, hence $p_{2k} = 0$ and $p_{2k+1} = 1$. Thus the pairs (1, 1) and (0, 0) can never occur.

If we reset the flip-flop after the arrival of each packet then the pair probabilities are:

$$\text{Prob}\{(1,1)\} = (\tfrac{1}{2} + \epsilon)^2 = \tfrac{1}{4} + \epsilon + \epsilon^2$$

$$\text{Prob}\{(1,0)\} = (\tfrac{1}{2} + \epsilon)(\tfrac{1}{2} - \epsilon) = \tfrac{1}{4} - \epsilon^2$$

$$\text{Prob}\{(0,1)\} = (\tfrac{1}{2} - \epsilon)(\tfrac{1}{2} + \epsilon) = \tfrac{1}{4} - \epsilon^2$$

$$\text{Prob}\{(0,0)\} = (\tfrac{1}{2} - \epsilon)^2 = \tfrac{1}{4} - \epsilon + \epsilon^2.$$

Comparison of these probabilities with those of the "not reset" situation shows that two of the pair probabilities are improved by resetting while two have been biased a little more.

Consideration of the probabilities associated with n-tuples shows that even for $|\epsilon|$ small some of the probabilities may deviate considerably from the desired values.

To obtain some idea of the bias, a long count of ones was made on each unit. This count was made under the reset situation. A typical result for one unit is $p^* = .499989140$ based on a total sample of 5.2^{26}. The results indicate that ϵ is very small.

Navy Electronics Laboratory
Report 1152

AN ELECTRONIC GENERATOR OF RANDOM NUMBERS, by G. M. Dillard and R. E. Simmons. 24 p., 21 December 1962.

UNCLASSIFIED

An electronic generator of random numbers has been constructed and evaluated. The device has been used to generate a sequence of ones and zeros with a predetermined probability of a one in the evaluation of an experimental sequential detector, and also to generate random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at NEL. Results of laboratory experiments employing the generator are described.

1. Random number generation

I. Dillard, G. M.
II. Simmons, R. E.

AD 01401
SF 001 02 05, Task 6072
(NEL D1-9)
This card is UNCLASSIFIED

Navy Electronics Laboratory
Report 1152

AN ELECTRONIC GENERATOR OF RANDOM NUMBERS, by G. M. Dillard and R. E. Simmons. 24 p., 21 December 1962.

UNCLASSIFIED

An electronic generator of random numbers has been constructed and evaluated. The device has been used to generate a sequence of ones and zeros with a predetermined probability of a one in the evaluation of an experimental sequential detector, and also to generate random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at NEL. Results of laboratory experiments employing the generator are described.

1. Random number generation

I. Dillard, G. M.
II. Simmons, R. E.

AD 01401
SF 001 02 05, Task 6072
(NEL D1-9)
This card is UNCLASSIFIED

Navy Electronics Laboratory
Report 1152

AN ELECTRONIC GENERATOR OF RANDOM NUMBERS, by G. M. Dillard and R. E. Simmons. 24 p., 21 December 1962.

UNCLASSIFIED

An electronic generator of random numbers has been constructed and evaluated. The device has been used to generate a sequence of ones and zeros with a predetermined probability of a one in the evaluation of an experimental sequential detector, and also to generate random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at NEL. Results of laboratory experiments employing the generator are described.

1. Random number generation

I. Dillard, G. M.
II. Simmons, R. E.

AD 01401
SF 001 02 05, Task 6072
(NEL D1-9)
This card is UNCLASSIFIED

Navy Electronics Laboratory
Report 1152

AN ELECTRONIC GENERATOR OF RANDOM NUMBERS, by G. M. Dillard and R. E. Simmons. 24 p., 21 December 1962.

UNCLASSIFIED

An electronic generator of random numbers has been constructed and evaluated. The device has been used to generate a sequence of ones and zeros with a predetermined probability of a one in the evaluation of an experimental sequential detector, and also to generate random sequences of ones and zeros in simulating the input to an experimental track-before-detect system being developed at NEL. Results of laboratory experiments employing the generator are described.

1. Random number generation

I. Dillard, G. M.
II. Simmons, R. E.

AD 01401
SF 001 02 05, Task 6072
(NEL D1-9)
This card is UNCLASSIFIED

INITIAL DISTRIBUTION LIST

Chief, Bureau of Ships
Code 320 Code 335 (3)
Code 360 (2) Code 670 (2)
Code 684 (2)
Bureau of Naval Weapons
DLI-3 DLI-31
RUDC-2 RUDC-11
R-56
Chief of Naval Personnel
Library
Chief of Naval Operations
Op-07T OP-94G43
Op-03EG
Chief of Naval Research
Code 455
Commander in Chief, Pac Flt
Commander in Chief, Lant Flt
Commander Operational Test &
Evaluation Force
Deputy Commander, Operational
Test & Evaluation Force, Pacific
Commander, Cruiser-Destroyer For,
Pac Flt Lant Flt
Destroyer Development Group, Pac
Commander Training Command,
Pac Flt
Commander Amphibious For,
Pac Flt (2)
Commander Service For, Lant Flt
Naval Air Development Center,
Library
Naval Missile Center
Tech. Library Code N3232
Naval Air Test Center, NANEP
Naval Ordnance Lab., Library
Naval Ordnance Test Station,
Pasadena Annex Library
Naval Ordnance Test Station,
China Lake
Naval Weapons Laboratory
Naval Radiological Defense Lab
David Taylor Model Basin
Navy Mine Defense Laboratory
Navy Underwater Sound Laboratory
Library (3)
ASW Tactical School, Lant Flt
Naval Engineering Experiment Sta
Library
Naval Research Laboratory
Code 5330 Code 2027
Code 5120 Code 5400
Naval Ordnance Laboratory, Corona
Navy Underwater Sound Reference Lab
Library
Air Development Squadron ONE (VX-1)
Beach Jumper Unit ONE
Beach Jumper Unit TWO
Office of Naval Research, Pasadena
Naval Submarine Base, New London
Electronic Officer
Naval Postgraduate School
Library (2)
Navy Representative
Project LINCOLN, MIT
Assistant SECNAV
Research and Development
DOD, Research & Engineering
Technical Library
Army Material Command
AMCRD-DE-E-S
Assistant Chief of Staff, G-2
US Army, IDB
Aberdeen Proving Ground, Tech Lib (2)
AMSTE-EL
Army Electronic Proving Ground
Technical Library
Redstone Scientific Information Center
Army Electronics R&D Laboratory
SELRA/SL-ADT SELRA/SR
Picatinny Arsenal
Army Research Office (Durham)
Electronic Development Activity,
White Sands
Army Transportation Terminal
Command, Pac
Army Air Defense Board, SUPPORT
Deputy Chief of Staff, Development, USAF
AFRST-EL/CS
Deputy Chief of Staff, Operations, USAF
AFOCC-C/I
Air Defense Command
ADOAC-DL ADOOA
Air Research & Development Command
SCSE
Air University, Library AUL3T-5028
Alaskan Air Command
Electronics (2)
Strategic Air Command
OAST
Air Force Missile Test Center
MU-135
Rome Air Development Center
RAALD
Wright Air Development Division
ASAPRD-Dist ASNVEG
ASROO-3
Federal Aviation Agency
NASA, Langley Research Center (3)
Air Weather Service, Scott AFB
National Bureau of Standards, Boulder
Bureau of Commercial Fisheries
Honolulu
U. S. Weather Bureau
Washington (2)
Weather Radar Lab, Oklahoma
National Security Agency (2)
Georgia Institute of Technology
New York University
Dept. of Meteorology & Oceanography
University of Miami
Marine Laboratory Library